DOJ Consumer Protection Unit Urges Delaware Consumers To Be On Guard Against IRS Scams And Other Financial Frauds

With IRS W-2 forms already issued by some employers, the 2018 tax season has arrived, and the Department of Justice Consumer Protection Unit is again warning Delaware consumers and employers to be on guard for fake IRS phone call scams and IRS Form W-2 email phishing scams that are targeting employers, including retail businesses, school districts, nonprofit organizations, and law firms.

IRS Phone Call Scam

In a typical IRS phone scam, a caller pretends to work for the Internal Revenue Service (or sometimes the U.S. Treasury Department), and tells the intended victim that the IRS will imminently be filing suit against the victim, or threatens the intended victim with arrest or some other kind of punishment, and the only way to avoid the lawsuit or arrest is to immediately pay a sum of money, usually via a pre-paid debit card or a money order, or even Amazon or iTunes gift cards.

“These scammers use scare tactics, threats, and aggressive language to put the person answering the phone into a precarious position,” said Attorney General Matt Denn. “They hope their prospective victims will quickly make payment in order to avoid the possibility of penalties like losing their jobs, or going to prison.”

The Internal Revenue Service says that these scammers often spoof the telephone number to disguise where they are calling from, and they sometimes manipulate the caller ID information so it seems like the call is coming from the IRS. They may

even give out a fake IRS badge number, and may even know the last four digits of a victim's Social Security number and try to use that information to gain a victim's trust.

As a reminder, the IRS will never reach out to a taxpayer with an initial contact by telephone, email, text message, or social media. The IRS also will never demand credit or debit card payment over the telephone, nor will the IRS demand that you pay a tax bill in a specific manner.

DOJ's Consumer Protection Unit urges consumers to ignore these calls and not return voicemail messages. Consumers should instead do the following:

- If you are worried that the call might be real, because you owe federal taxes, or think you might owe federal taxes, hang up and call the IRS directly at 1-800-829-1040. IRS workers there will be able to help you with any payment questions.
- Report the scam to federal authorities: fill out the "IRS Impersonation scam" form on TIGTA's website, or call TIGTA at 800-366-4484, and also consider filing a complaint with the Federal Trade Commission at www.ftc.gov (add "IRS Telephone Scam" to the comments in your complaint).

IRS Form W-2 Phishing Scam

Delawareans should also be aware of a dangerous email scam that has been circulating nationwide and is targeting a wide variety of public and private-sector employers, including retail businesses, universities, secondary school districts, nonprofit organizations, hospitals, and law firms. The scam first appeared in 2016, but saw a significant increase in 2017, with an estimated 200 employers across the United States being victimized last year.

Typically, the scammer sends a "spoofing" email posing as an internal executive or official within the organization,

requesting employee payroll data, including IRS W-2 forms that contain Social Security numbers and other personally identifiable information. If these cybercriminals are successful in tricking payroll and human resource officials into disclosing that data, they can use the data to file fraudulent tax returns for refunds and commit other forms of identity theft.

According to the IRS, these are examples of the details that may be contained in some of these emails:

- "Kindly send me the individual [2017] W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review."
- "Can you send me the updated list of employees with full details (Name, Social Security Number, Date of Birth, Home Address, Salary)."
- "I want you to send me the list of W-2 copy of employee wage and tax statement for [2017], I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap."

The IRS has also established a process that will allow employers and payroll service providers to quickly report any data losses related to this W-2 scam: https://www.irs.gov/individuals/form-w2-ssn-data-theft-information-for-businesses-and-payroll-service-providers. The IRS has established a dedicated email address for employers to report W-2 scams and data thefts: dataloss@irs.gov. According to the IRS, if notified in time the IRS can take steps to prevent employees from being victimized by identity thieves filing fraudulent returns in their names. There is also information about how to report receiving the scam email even if an employer did not fall victim to the scam.

DOJ also reminds employers that if they are victimized by this scam, they have suffered a data breach and may need to give notice to affected individuals under Delaware's data breach

notification law (Title 6, Chapter 12B of the Delaware Code), and may also need to give notice under other applicable state or federal law. Employers who suffer a data breach should consult with legal counsel to ensure compliance with all applicable data breach notification laws.